CMMC 2.0 and NIST SP 800-171 Compliance Training

Course: **00063**
Filter: **Beginner**
Duration: **2 days**
Category:: **Cloud Security**
Price: **2800,00 €**

About Course

Recent sweeping updates to the U.S. Department of Defense Cybersecurity Maturity Model Certification (CMMC) requirements have left the consultants, contractors, and the Defense Industrial Base (DIB) questioning where this leaves us and how to proceed. This course is intended to address the questions of what CMMC 2.0 is all about, how certification will work under the new model, the SP 800-171 requirements that must be satisfied and how to meet them, and what this means for DoD contracting organizations. These exact 800-171 requirements cover all Non-Federal Organizations (NFOs) that handle U.S. Federal Government controlled unclassified information. This course will also feature self-attestation guidance and will help organizations meet the external 3rd party assessments that will still be required for a subset of businesses handling protected U.S. Federal Government information.

What you'll learn

- Understand and comply with the new CMMC 2.0 framework
- Assess CMMC 2.0 and CMMC 1.0 differences and repercussions to your organization
- Meet NIST SP 800-171 requirements
- Perform self-assessments conforming to DFARS standards and generate a SPRS score
- Satisfy third-party CMMC 2.0/SP 800-171 assessments
- Maintain an acceptable security posture over the contract lifecycle
- Continue learning and face new challenges with after-course one-on-one instructor coaching

Pre-requisites

- Prior security experience is helpful but not necessary. Critical thinking skills and the ability to make decisions are key.

Curriculum

Module 1: The Nature of Protected Information

- Acknowledging the importance of protecting US Government information
- Recognizing categories of protected information
- Describing protected information and the law

Module 2: Threats to Protected Information

- Defining types of security failures
- Judging the impact of security failures
- Defining risk
- Identifying threats and vulnerabilities in organizational systems
- Recognizing motivations for data compromise
- Identifying characteristics of threat actors

Module 3: Introduction to CMMC 2.0

- Describing CMMC Goals
- Synopsizing CMMC Evolution
- Describing the four CMMC 2.0 program phasesDefining the model tiers
- Listing assessment requirements
- Explaining model implementation
- Charting the CMMC implementation timeline

Module 4: CMMC 2.0 and NIST SP 800-171

- Describing NIST SP 800-171, SP 800-171A, and SP 800-172

- Categorizing security controls
- Identifying SP 800-171 control families
- Describing SP 800-171 security control structure
- Explaining the importance of basic assumptions underlying SP 800-171

Module 5: Characterizing the Non-Federal System

- Identifying NARA CUI categories and markings
- Verifying confidentiality impact level
- Identifying special considerations for classified defense information
- Determining the organizational system boundary
- Building the System Security Plan

Module 6: Securing the Organizational System

- Determining the security control baseline
- Assessing the need for enhanced assurance
- Updating the System Security Plan
- Tailoring the security control baseline
- Selecting the approach to securing organizational systems
- Implementing security controls
- Documenting security control implementation, compliance, and effectiveness

Module 7: Assessing System Cybersecurity Risk

- Building the Security Assessment Plan
- Assessment methodologies
- Assessment optimization
- Assessing security control compliance and effectiveness
- Documenting security control compliance

Module 8: Reporting Self-Assessment Results

- Completing the System Security Plan
- Building the Plan of Action and Milestones (POA&M)
- Requesting CMMC waivers
- Compiling the assessment report

- Preserving an acceptable system security posture